AO93 Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of 6815 East Camelback Road, Apt #1010, Scottsdale, AZ 85251.	Case No. 21-369 MB **(Filed Under Seal)**

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before December 28, 2021 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

N/A ☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days (*not to exceed 30*) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 12-14-2021 @ 1 pm

Judge's signature

City and state: Phoenix, Arizona

Honorable Michelle H. Burns, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

6815 East Camelback Road #1010, Scottsdale, Arizona, 85251

The entire premises of apartment number 1010, located at 6815 East Camelback Road, Scottsdale, Arizona, 85251. This address is part of the Optima Sonoran Village complex that encompasses multiple land parcels.

The address known as 6815 East Camelback Road, Scottsdale, Arizona is a multi-story apartment building located on the southeast corner of Camelback Road and 68th Street in Scottsdale, Arizona. Apartment 1010 is located on the first floor, northwest corner, of the building. The door to apartment 1010 is inside of a secure area and located on the southeast portion of the unit facing to the south. Affixed to the door is a decorative peephole bearing the numbers "1-0-1-0" in black lettering.

ATTACHMENT "B"

ITEMS TO BE SEIZED

1. Any records pertaining to the Paycheck Protection Program (PPP) or Economic Injury Disaster Loans (EIDL) from 2020 or 2021.
    a. Loan applications/agreements
    b. Correspondence with the Small Business Administration or private lenders
    c. Notes or ledgers pertaining to PPP or EIDL loan submissions or the receipt of loan funds
2. Records from financial institutions from 2019, 2020, and 2021.
    a. Account opening documents
    b. Bank statements
    c. All funds and credits, including cryptocurrencies, private keys and recovery seeds, stored in or accessible via cryptocurrency wallets
3. Records pertaining to the formation and operation of business entities.
    a. Corporation filings
    b. Employee payroll records
    c. Receipts for business expenses
    d. Invoices or other proof of sales
    e. Tax documents to include business formation, employee wages, and tax returns.
4. Any records, communications, and information relating to a conspiracy to submit fraudulent PPP and EIDL applications.
5. Any electronic devices that can store and send information digitally to include cellular telephones, smart phones, tablets, computers, and electronic media storage devices.

6. Records relating to transactions involving digital assets or digital currency, including date of transaction, amount, and name of exchange (e.g., Coinbase, Kraken).
7. Records, receipts, and information relating to any purchases occurring between March 1, 2020, to present including investments, property and/or vehicle deeds and/or titles.
8. Articles of personal property tending to establish the identity of persons who have dominion and control over 6815 East Camelback Road #1010, Scottsdale, Arizona, 85251, or items to be seized, including but not limited to: rent receipts, utility payments, utility bills, telephone bills, miscellaneous addressed mail, personal letters, personal identification, keys, purchase receipts, sale receipts, tax statements, photographs, and vehicle registrations.
9. Any/all currency (United States Federal Reserve notes and/or foreign currency) as well as cashier's checks, promissory notes, bonds, any/all negotiable instruments.
10. Passwords, encryption keys, passcodes, and other access devices that may be necessary to access secured areas, items, or things otherwise listed in the search warrant and located at 6815 East Camelback Road #1010, Scottsdale, Arizona, 85251.

AO 106 Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
District of Arizona

In the Matter of the Search of 6815 East Camelback Road, Apt #1010, Scottsdale, AZ 85251.	Case No. 21-369MB

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

As further described in Attachment A

located in the District of Arizona, there is now concealed:

As set forth in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code/Section	*Offense Description*
18 U.S.C. § 1343	Wire Fraud
18 U.S.C. § 1957(a)	Transactional Money Laundering
18 U.S.C. § 371	Conspiracy

The application is based on these facts:

See attached Affidavit of Special Agent Seth H. Thompson

☒ Continued on the attached sheet.

☐ Delayed notice of 30 days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Reviewed by AUSA Raymond K. Woo RW

Applicant's Signature

Seth H. Thompson, Special Agent, HSI
Printed name and title

Sworn and subscribed to me telephonically.

Date: 12-14-2021

Judge's signature

City and state: Phoenix, Arizona

Honorable Michelle H. Burns, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

PROPERTY TO BE SEARCHED

6815 East Camelback Road #1010, Scottsdale, Arizona, 85251

The entire premises of apartment number 1010, located at 6815 East Camelback Road, Scottsdale, Arizona, 85251. This address is part of the Optima Sonoran Village complex that encompasses multiple land parcels.

The address known as 6815 East Camelback Road, Scottsdale, Arizona is a multi-story apartment building located on the southeast corner of Camelback Road and 68th Street in Scottsdale, Arizona. Apartment 1010 is located on the first floor, northwest corner, of the building. The door to apartment 1010 is inside of a secure area and located on the southeast portion of the unit facing to the south. Affixed to the door is a decorative peephole bearing the numbers "1-0-1-0" in black lettering.

ATTACHMENT "B"

ITEMS TO BE SEIZED

1. Any records pertaining to the Paycheck Protection Program (PPP) or Economic Injury Disaster Loans (EIDL) from 2020 or 2021.
    a. Loan applications/agreements
    b. Correspondence with the Small Business Administration or private lenders
    c. Notes or ledgers pertaining to PPP or EIDL loan submissions or the receipt of loan funds
2. Records from financial institutions from 2019, 2020, and 2021.
    a. Account opening documents
    b. Bank statements
    c. All funds and credits, including cryptocurrencies, private keys and recovery seeds, stored in or accessible via cryptocurrency wallets
3. Records pertaining to the formation and operation of business entities.
    a. Corporation filings
    b. Employee payroll records
    c. Receipts for business expenses
    d. Invoices or other proof of sales
    e. Tax documents to include business formation, employee wages, and tax returns.
4. Any records, communications, and information relating to a conspiracy to submit fraudulent PPP and EIDL applications.
5. Any electronic devices that can store and send information digitally to include cellular telephones, smart phones, tablets, computers, and electronic media storage devices.

6. Records relating to transactions involving digital assets or digital currency, including date of transaction, amount, and name of exchange (e.g., Coinbase, Kraken).
7. Records, receipts, and information relating to any purchases occurring between March 1, 2020, to present including investments, property and/or vehicle deeds and/or titles.
8. Articles of personal property tending to establish the identity of persons who have dominion and control over 6815 East Camelback Road #1010, Scottsdale, Arizona, 85251, or items to be seized, including but not limited to: rent receipts, utility payments, utility bills, telephone bills, miscellaneous addressed mail, personal letters, personal identification, keys, purchase receipts, sale receipts, tax statements, photographs, and vehicle registrations.
9. Any/all currency (United States Federal Reserve notes and/or foreign currency) as well as cashier's checks, promissory notes, bonds, any/all negotiable instruments.
10. Passwords, encryption keys, passcodes, and other access devices that may be necessary to access secured areas, items, or things otherwise listed in the search warrant and located at 6815 East Camelback Road #1010, Scottsdale, Arizona, 85251.

ATTACHMENT C

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Seth H. Thompson, being duly sworn, depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations (hereinafter, "HSI"). As such, I am an investigator or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), who is empowered to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code.

2. I have been employed as a Special Agent with HSI since December, 2009. I attended the Federal Law Enforcement Training Center, in Brunswick, Georgia, where I received investigative training in areas including, but not limited to, narcotics smuggling, human smuggling/trafficking, financial investigations, and cyber crimes. This training consisted of approximately 496 hours of basic law-enforcement training and 456 hours of comprehensive classroom training in different investigative techniques.

3. Prior to my position as a Special Agent with HSI, I was employed full time with the Arizona National Guard's Joint Counter Narco-Terrorism Task Force as an intelligence analyst for seven years. During that time, I was assigned to work with the Phoenix Police Department and then with ICE Office of Investigations. In

2008, I received a Bachelor of Science degree in Political Science from Arizona State University.

4. During my employment as a Special Agent with HSI, I have participated in investigations involving, but not limited to, smuggling, narcotics manufacturing and distribution, money laundering, and financial fraud. These investigations have resulted in the seizure of illicit drugs, currency, firearms, and real property. During these investigations, I have participated in interviewing witnesses and cooperating sources and have read official reports of similar interviews by other officers. I have also participated in surveillance operations to observe and record movements of persons suspected of being involved in criminal activity.

5. Through my investigations, training, experience, and discussions with other law enforcement personnel, I have become familiar with the tactics and methods used by individuals to commit fraud as well as the tactics used to launder the proceeds from fraudulent schemes.

II. PURPOSE OF AFFIDAVIT

6. I make this Affidavit in support of an application for a search warrant for the premises located at 6815 East Camelback Road, Apt #1010, Scottsdale, AZ 85251. This location is further described in **Attachment A.**

7. Because this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to

establish probable cause to believe that evidence of a violation of Title 18, United States Code, Section 1343, Wire Fraud, a violation of Title 18, United States Code, Section 1957(a), Transactional Money Laundering, and a violation of Title 18, United States Code, Section 371, Conspiracy, are presently contained at 6815 East Camelback Road #1010, Scottsdale, AZ 85251 as described in **Attachment B**.

8. Based on my involvement in this investigation and my review of reports and information provided to me by Special Agents from the United States Secret Service (hereinafter "USSS"), I am familiar with the circumstances of this investigation.

III. BACKGROUND REGARDING CARES ACT

9. The Coronavirus Aid, Relief, and Economic Security (hereinafter "CARES") Act was enacted in March 2020 to provide emergency financial assistance to the millions of Americans who were suffering the economic effects caused by the COVID-19 pandemic.

10. The CARES Act authorized the Small Business Administration (hereinafter "SBA") to provide eligible small businesses with Economic Injury Disaster Loans (hereinafter "EIDL"). The EIDL program was established to provide low-interest loans to small businesses experiencing substantial disruption from declared disasters. The declared disaster date for the COVID-19 pandemic is January 31, 2020. Small businesses applying for an EIDL under the CARES Act must have been operating prior to this date.

11. Through EIDL, applicants can be issued an advance of up to $10,000. This amount is determined by the number of employees the applicant certified as employing as of January 31, 2020. The advance was not required to be repaid.

12. Small businesses could also apply for an EIDL if they were operating prior to the disaster date, and they had 500 or fewer employees.

13. In order to obtain and EIDL, a business was required to submit an application to the SBA and provide information about its operation, to include business name, date of business establishment, number of employees as of January 31, 2020, gross revenue for the twelve months preceding the disaster, and cost of goods sold in the twelve months preceding the disaster. If the application was approved, the loan amount was determined in part by the information provided regarding the gross revenues and the cost of goods sold. These loans were funded directly from the SBA.

14. The CARES Act also created the Paycheck Protection Program (hereinafter ("PPP"), which provided businesses with forgivable loans to be used for job retention and certain other expenses. Like EIDL, businesses applying for PPP loans were required to provide certain business information, including number of employees and average payroll costs. Unlike EIDL, PPP loans were funded by participating lenders.

IV. STATEMENT OF PROBABLE CAUSE

15. In February 2021, Your Affiant became aware of an individual residing in Scottsdale, AZ named Ernest Lerma (hereinafter "LERMA") suspected

of having fraudulently received Economic Injury Disaster Loan (hereinafter "EIDL") funds from the Small Business Administration (hereinafter "SBA"). These loans were made available by the SBA to businesses affected by the Covid-19 pandemic.

16. Investigation into LERMA revealed that he formed a corporation in Arizona called Bluejay Secrets, LLC on April 7, 2020.

17. On April 2, 2021, SA Thompson received records from Alaska USA Federal Credit Union for account 4934906 belonging to Bluejay Secrets in which LERMA is the only signer.

18. A review of these records revealed the account had received large deposits from several business entities between July 2020 and September 2020. It was also discovered that there were large payments made from the account to an entity called Seguros Y Mas during the same period.

19. Further investigation revealed Seguros Y Mas, LLC is an Arizona-based corporation owned by Nino Mihilli (hereinafter "MIHILLI"). It was found that MIHILLI was the subject of a USSS investigation in which he was believed to have conspired with others to fraudulently obtain EIDL and Paycheck Protection Program (hereinafter "PPP") loans.

20. The USSS investigation found that MIHILLI and at least two co-conspirators likely recruited numerous individuals to provide business names and bank accounts to be used for the purpose of submitting fraudulent EIDL and PPP loan applications in their own names. Once those individuals received the

fraudulent loan funds from the SBA, or a private lender in the case of PPP loans, they would pay a portion of those funds to their recruiter, who would then pay a portion of those funds to MIHILLI. It is believed MIHILLI was typically the one who prepared the fraudulent loan applications due to the fact that most of the IP addresses used to submit the applications were registered to him or to companies owned by him.

21. In August 2021, your Affiant was provided with copies of EIDL applications from the SBA that revealed each of the business entities who had sent Bluejay Secrets, LLC large sums of money had each received EIDL funds beforehand. In addition, the SBA provided your Affiant with two EIDL applications submitted on behalf of an Arizona-based corporation owned by LERMA called Squabble, LLC.

22. On July 1, 2020, LERMA electronically submitted an EIDL application to the SBA on behalf of Squabble, LLC. The application claimed that in 2019, the corporation received $300,005 in gross earnings, had $100,000 in cost of goods sold, and employed fifteen employees. Your Affiant received records for two bank accounts belonging to Squabble, LLC, both of which were not opened until 2020. Certified records provided by the Arizona Department of Economic Security (hereinafter "DES") found that there were no reported employee wages for Squabble, LLC in 2019 or 2020. This loan application was ultimately denied by the SBA.

23. On July 2, 2020, LERMA electronically submitted a second EIDL application to the SBA on behalf of Squabble, LLC. This application claimed that in 2019 the company had gross earnings of $300,000, cost of goods sold of $10,000, and ten employees. This application was also denied by the SBA.

24. On July 21, 2020, Daniel Bahena Ortiz (hereinafter "BAHENA ORTIZ) electronically submitted an EIDL application to the SBA on behalf of The Engineur, LLC, an Arizona-based corporation owned by BAHENA ORTIZ. The Certificate of Completion for the application was submitted using an IP address registered to MIHILLI. The application claimed that in 2019, the corporation had gross earnings of $850,000, cost of goods sold of $400,000, and ten employees.

25. As part of the EIDL application, BAHNEA ORTIZ provided a Bank of America bank account belonging to the Engineur, LLC. A review of this account found that in the twelve months prior to January 31, 2020 (date of disaster established by the SBA; qualifying applicant businesses must have existed prior to this date), the account only received a total of $585. Arizona DES records show that there were no employee wages reported for The Engineur, LLC in 2019 or 2020.

26. On July 22, 2020, the SBA approved an EIDL for The Engineur, LLC in the amount of $150,000 and on July 23, 2020, The Engineur, LLC bank account received a deposit from the SBA in the amount of $149,900 (minus $100 processing fee). On July 27, 2020, a $30,000 cashier's check was drawn from the account and made payable to Bluejay Secrets, LLC.

27. On July 23, 2020, Stephen Dison (hereinafter "DISON") electronically submitted an EIDL application to the SBA on behalf of Three Ball Climbing, LLC, an Arizona-based corporation owned by DISON. The Certificate of Completion for the application was submitted using an IP address registered to a company owned by MIHILLI. The application claimed that in 2019 the company had gross earnings of $950,000, cost of goods sold of $400,000, and twelve employees.

28. As part of the EIDL application, DISON provided a JPMorgan Chase bank account belonging to Three Ball Climbing, LLC. A review of this account found that in the twelve months prior to January 31, 2020, the account received a total of only $117,000 in deposits. Arizona DES records show that there were no employee wages reported for Three Ball Climbing, LLC in 2019 or 2020.

29. On August 6, 2020, the EIDL for Three Ball Climbing, LLC was approved by the SBA and on August 10, 2020, the Three Ball Climbing, LLC bank account received a deposit from the SBA in the amount of $149,900. On or about August 18, 2020, a $30,000 business check was withdrawn from the account made payable to Bluejay Secrets, LLC.

30. On July 24, 2020, BAHENA ORTIZ electronically submitted a an EIDL application to the SBA on behalf of USA Fast, LLC, an Arizona-based corporation owned by BAHENA ORTIZ. The Certificate of Completion for the application was submitted using an IP address registered to a company owned by

MIHILLI. The application claimed that in 2019, the corporation had gross earnings of $950,000, cost of goods sold of $400,000, and twelve employees.

31. As part of the EIDL application, BAHENA ORTIZ provided a Bank of America bank account belonging to USA Fast, LLC. A review of this account found that from account opening on July 9, 2019 to January 31, 2020 the account received a total of only $5,614.93. Arizona DES records found that no employee wages were reported for USA Fast, LLC in 2019 or 2020.

32. On July 24, 2020, an EIDL for USA Fast, LLC was approved by the SBA for the amount of $150,000 and on July 28, 2020, the USA Fast, LLC account received a deposit from the SBA in the amount of $149,900. On July 30, 2020, $30,000 was electronically transferred from USA Fast, LLC to Bluejay Secrets, LLC.

33. On August 5, 2020, Vanessa Ortiz (hereinafter "ORTIZ") electronically submitted an EIDL application to the SBA on behalf of Urban Goods, LLC, an Arizona-based corporation owned by ORTIZ. The application was submitted using an IP address registered to a company belonging to MIHILLI. The application claimed that in 2019, the corporation had gross earnings of $700,000, cost of goods sold of $350,000, and ten employees.

34. As part of the EIDL application, ORTIZ provided a Desert Financial Credit Union account belonging to Urban Goods, LLC. The bank account was opened on August 5, 2020 (same day EIDL application was submitted) with a zero

balance. Arizona DES records show that there were no employee wages reported for Urban Goods, LLC in 2019 or 2020.

35. On August 5, 2020, an EIDL for Urban Goods, LLC was approved for the amount of $150,000, and on August 7, 2020, the Urban Goods, LLC account received a deposit from the SBA in the amount of $149,900. On August 11, 2020, $30,000 was electronically transferred from Urban Goods, LLC to Bluejay Secrets, LLC.

36. On August 5, 2020, Brandon Hearvey (Hereinafter "HEARVEY") electronically submitted an EIDL application to the SBA on behalf of Rammi Scott, LLC, an Arizona-based corporation that HEARVEY is a member of. The application was submitted using an IP address previously used by LERMA to electronically submit an unemployment benefit claim to the State of Arizona. The application for Rammi Scott, LLC claimed that in 2019, the corporation had gross earnings of $800,000, cost of goods sold of $25,000, and eight employees.

37. As part of the EIDL application, HEARVEY provided a JPMorgan Chase bank account belonging to Rammi Scott, LLC. The bank account was opened on July 28, 2020. Arizona DES records show that there were no employee wages reported for Rammi Scott, LLC in 2019 or 2020.

38. On August 10, 2020, an EIDL was approved by the SBA for Rammi Scott, LLC for the amount of $150,000, and on August 12, 2020, the Rammi Scott, LLC account received a deposit from the SBA in the amount of $149,900. On

August 12, 2020, a cashier's check was withdrawn from the account in the amount of $18,000 made payable to Bluejay Secrets, LLC.

39. On August 18, 2020, Robert Adams III (hereinafter "ADAMS") electronically submitted an EIDL application on behalf of 007 Ventures, LLC, an Arizona-based corporation owned by ADAMS. The Certificate of Completion for the application was submitted using an IP address registered to MIHILLI. The application claimed that in 2019, the corporation had gross earnings of $700,000, cost of goods sold of $350,000, and nine employees.

40. As part of the EIDL application, ADAMS provided a Wells Fargo bank account belonging to 007 Ventures, LLC. A review of this account found that from October 2, 2019 when the account was opened, to January 31, 2020, the account received a total of only $8,300. Arizona DES records show that there were no employee wages reported for 007 Ventures, LLC in 2019 or 2020.

41. On August 31, 2020, an EIDL for 007 Ventures, LLC was approved by the SBA for the amount of $150,000, and on September 2, 2020, the account for 007 Ventures, LLC received a deposit from the SBA in the amount of 149,900. Also on September 2, 2020, a $30,000 electronic transfer was made from 007 Ventures, LLC to Bluejay Secrets, LLC.

42. On August 20, 2020, Ariana Vazquez (hereinafter "VAZQUEZ") electronically submitted an EIDL application on behalf of Wet Haute Couture, LLC, an Arizona-based corporation owned by VAZQUEZ. The application was submitted using an IP address registered to a company owned by MIHILLI. The

application claimed that in 2019, the corporation had gross sales of $950,000, cost of goods sold of $400,000, and seven employees.

43. As part of the EIDL application, VAZQUEZ provided a Wells Fargo bank account belonging to Wet Haute Couture, LLC. A review of this account found that in the twelve months prior to January 31, 2020, a total of only $35,563.31 was deposited into the account. Arizona DES records found that there were no employee wages reported for Wet Haute Couture, LLC in 2019 or 2020.

44. On September 4, 2020, an EIDL for Wet Haute Couture, LLC was approved by the SBA for the amount of $150,000, and on September 9, 2020, the account for Wet Haute Couture, LLC received a deposit from the SBA in the amount of $149,900. Also on September 9, 2020, a $30,000 electronic transfer was made from Wet Haute Couture, LLC to Bluejay Secrets, LLC.

45. Between July 29, 2020 and September 14, 2020, LERMA made five payments utilizing the Bluejay Secrets, LLC bank account to MIHILLI's Seguros Y Mas bank account totaling $108,500.

46. On or about October 28, 2021, co-conspirator B.R. was interviewed by law enforcement in the District of Nevada. B.R. had previously submitted a PPP loan for his company ATeam NV LLC. B.R. confirmed he was assisted by NIKOLAS MIHILLI (who is the brother of MIHILLI) in applying for a PPP loan on May 29, 2020 that contained false information and documentation. B.R. also confirmed that he met MIHILLI through NIKOLAS MIHILLI.

47. B.R.'s company, ATeam NV LLC, was approved for a PPP loan of approximately 1.5 million. NIKOLAS MIHILLI instructed B.R. to pay portions of the loan to people who assisted B.R., which included himself, MIHILLI, and to D.B. An IP address belonging to MIHILLI was used to submit part of the PPP loan for B.R.

48. On or about June 13, 2020, a $150,581 cashier's check from B.R. was deposited into NIKOLAS MIHILLI's bank account.

49. On or about June 16, 2020, a $150227 cashier's check from B.R. was deposited into MIHILLI's bank account.

50. A review of telephone records for 480-270-2105, a number registered to LERMA, found that between April 13, 2020 and July 7, 2020, LERMA communicated with MIHILLI on thirteen different days. Then beginning on July 8, 2020, communication between the two became much more frequent. This corresponds with the approximate time period (July 21, 2020) that loans began to be submitted by individuals recruited by LERMA.

51. On December 1, 2021, SA Tony Bueno served a DHS Summons to the property management office at Optima Sonoran Village. This is the apartment complex in which LERMA was believed to reside. Upon receipt of the Summons, a leasing agent of Optima Sonoran Village confirmed that LERMA currently resides at 6815 East Camelback Road, Apt #1010, Scottsdale, AZ. Furthermore, the leasing agent also provided SA Bueno with a copy of the lease agreement that states the same.

52. Because the EIDL and PPP loan application processes were done electronically, it is likely that evidence of fraud is still stored on electronic devices located in LERMA's residence. This stored evidence could likely include copies of loan applications/agreements, records of electronic funds transfers, correspondence with the SBA and other lenders, and correspondence between co-conspirators. It is also reasonable to believe physical copies of financial documents and documents related to the formation and operation of business entities controlled by LERMA will also be stored at his residence.

V. COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

52. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

53. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage

medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence,

because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

50. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional

information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed,

thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last,

information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information

necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain unauthorized access to a victim computer, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

53. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premise for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the PREMISES, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on a premise could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things

described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

54. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging,

or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

VI. CONCLUSION

55. Based on the forgoing, I respectfully request that this Court issue a search warrant for 6815 East Camelback Road #1010, Scottsdale, AZ 85251 (**Attachment A**) for the items to be seized listed in **Attachment B**, as evidence relating to the commission of criminal offenses in violation of Title 18, United States Code, Section 1343, Title 18, United States Code, Section 1957(a), and Title 18, United States Code, Section 371.

SETH H. THOMPSON
Special Agent
Homeland Security Investigations

Telephonically subscribed and sworn to me on the 14 day of December, 2021.

HONORABLE MICHELLE H. BURNS
United States Magistrate Judge